The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
4/14/2010

SUBJECT:
Vulnerability in Cisco Security Desktop Could Allow Remote Code Execution

OVERVIEW:
A vulnerability exists in an ActiveX control on Cisco Secure Desktop (CSD) that will allow an attacker to download malicious files. CSD is a tool provided by Cisco to extend the security of Secure Socket Layer Virtual Private Networks (SSL VPN) to a user's work station. ActiveX controls are small programs or animations that are downloaded or embedded in Web pages which will typically enhance functionality and user experience. Secure Socket Layer (SSL) is a protocol used for transmitting documents securely via the Internet. SSL is the most widely used protocol for secure network communication. A Virtual Private Network (VPN) permits secure, encrypted connections between a company's private network and remote users.

This vulnerability can be exploited if a user visits a specially crafted webpage hosting a malicious file designed to take advantage of the vulnerability. Successful exploitation may result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Cisco Secure Desktop versions prior to 3.5.841

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: N/A

DESCRIPTION:
The Cisco Secure Desktop (CSD) is prone to a vulnerability in an Active X control that allows an attacker to download a malicious file. To leverage this technology the software must communicate with a Cisco ASA, router, VPN appliance or WebVPN module on Catalyst 6500 or 7500 routers. The Active X control is a Cisco signed control that is used during the installation process. This control fails to properly validate the integrity of an executable file that is downloaded during the installation process. An attacker could modify this executable file to add the malicious content; the file would then be executed with the privileges of the logged in user.

To leverage this issue the attacker builds a webpage that hosts the malicious file. The end user must then visit the malicious page at which time the file will be downloaded and executed on the users system. Successful exploitation may result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Cisco to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Cisco:

http://www.cisco.com/en/US/products/products_security_advisory09186a0080b25d01.shtml
http://www.cisco.com/en/US/docs/security/csd/csd342/release/notes/csdrn342.html

Security Focus:

http://www.securityfocus.com/bid/39478